Kentucky.gov

Commonwealth Office of Technology

From: Ritchey, Gail (COT)
Sent: Friday, June 13, 2008 1:40 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: Targeted Phishing Attempts

COT Security Alert

Phishing emails have arrived recently in state inboxes in greater numbers, especially those using the Commonwealth Credit Union as their cover. By posing to be a familiar local institution, the phishers hope to gain the trust of recipients and obtain personal information. The goal of a phishing email is to entice the recipient through fear or other social manipulation into clicking on a link, or in the case of vishing calling a number, and divulging personal information. The personal information can then be used by the phisher to commit fraud by opening accounts in the recipient's name, by accessing existing accounts and by other illegal activities. The Commonwealth Credit Union posts information concerning phishing attempts against their customers on their website at http://www.cwcu.org/library/IDtheft/index.htm.

By reporting phishing emails properly, many emails can be stopped before they reach more inboxes. Sending the phishing email as an attachment gives the most useful information for blocking. For assistance in reporting phishing emails, contact the COT Security Administration Branch, COTSecurityServicesISS@ky.gov. The phishing email should be completely deleted from the inbox, deleted items box and sent box once the incident is reported.

Users should be aware that banks and other financial institutions **do not use email** to alert customers of issues with accounts or request personal information in any way. If customers feel the need to check on their account, they should **initiate** a phone call using the number listed in the public phone book for that institution, access an existing online account, or visit the institution in person. Information in phishing emails must **never** be used in any way.

User awareness is an essential part of defense against phishing. For more information about the dangers of phishing emails see http://www.microsoft.com/protect/yourself/phishing/identify.mspx or http://onguardonline.gov/phishing.html.

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Commonwealth Office of Technology
Security Administration Branch
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServices@ky.gov
http://cot.ky.gov/security/